CHAPTER 7

Implementation of Network Management

Cisco Network Assistant

Cisco Network Assistant (CNA) is a PC-based network management application optimized for wired and wireless LANs. It simplifies configuration, deployment, and ongoing management of networks. CNA is available at no cost and can be downloaded from http://www.cisco.com/go/cna. CNA gives a centralized network view through a user-friendly GUI for configuration, monitoring, troubleshooting, and maintenance. It allows network administrators to easily apply common services, generate inventory reports, synchronize passwords, upgrade software, and employ features across Cisco switches, routers, and access points.

CNA uses the concept of the community to group the switches and routers in the network. In each community, candidates are network devices that have IP addresses but are not part of a community. Members are network devices that are currently part of a community. To join a community, a candidate must meet the following requirements:

- The candidate has an IP address.
- Cisco Discovery Protocol (CDP) version 2 is enabled (the default) if you want the device to be autodiscovered.
- The candidate has HTTP (or HTTPS) enabled.

CNA uses CDP to automatically discover all the available devices in the network. Beginning with the IP address for a starting device and the port numbers for HTTP (or HTTPS) protocols, CNA uses CDP to compile a list of community candidates that neighbor the starting device. CNA can discover candidate and member devices across multiple networks and VLANs as long as they have valid IP addresses. By default, CNA in community mode discovers up to four hops away. If CNA fails to discover a device, you can add it manually through the IP management IP address.

The latest CNA release, version 5.1, can be installed on the following:

- Windows XP with Service Pack 1 or later
- Windows 2003 with Service Pack 1 or later
- Windows 2000 with Service Pack 3 or later

CNA supports networks with 40 or fewer switches and routers. Within each community, CNA supports up to 20 devices, including up to 4 Catalyst 4500 series switches (modular), 16 Catalyst 2900/3500 switches, 2 routers, and 2 PIX firewalls. The network components in EttF 1.1 that CNA 5.1 supports include those in the cell/area and manufacturing zones: Catalyst 2955, Catalyst 3750, and Catalyst 4500.

The server running CNA is recommended to be placed in the manufacturing zone (level 3).

The following three steps are needed to start using CNA:

1. Install the CNA application on the PC.
2. Configure HTTP or HTTPS on all the switches and routers that CNA will contact.
3. Launch CNA to connect to the switches and routers.

The detailed instructions of these procedures are available at the following URL: http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sg/configuration/guide/netasist.html#wp1080326

CNA Security Considerations

Note the following security considerations:

- Use HTTPS instead of HTTP for CNA access to routers and switches to ensure that the information exchanged between the web browser and CNA is encrypted.
- Because CDP is recommended to be disabled for security reasons, the operator can add routers and switches to the CNA device list manually.

Cisco Adaptive Security Device Manager

Cisco Adaptive Security Device Manager (ASDM) delivers security management and monitoring through an intuitive, easy-to-use web-based management interface. The ASDM accelerates security appliance deployment with intelligent wizards, robust administration tools, and versatile monitoring services that complement the Cisco ASA 5500 Series Adaptive Security Devices. The ADSM provides the following features:

- Packet tracer utility—Verifies the impact of real traffic flows on the entire system configuration. This utility sketches animated results as each policy is rigorously tested and provides direct links to correct failed tests for exploration-free policy tuning.
- Profile-based management for all application inspection and control capabilities—Uses preconfigured low, medium, and high security profiles for each of the application inspection engines for rapid deployment in any security environment. The ASDM enables the granular customization of any of the security profiles to cater to the needs of advanced applications. It provides easy integration of user-defined regular expressions into existing security policies to allow rapid threat mitigation against new and upcoming application attacks.
- High-availability and scalability wizard—Simplifies the deployment of active/active and active/standby high availability. It helps ensure comprehensive connectivity testing and error verification for smooth and accurate deployment.
- Integrated security policy and access control table—Enhances the policy configuration and management experience by providing a stream-lined, in-depth perspective into all the access rules, AAA, and security policies of the system. The ASDM facilitates rapid troubleshooting through a new rule query option that enables administrators to quickly search for network elements and the policies employing them. It enables the rapid editing of all network and service object groups via a new object group selector panel.
- Easy troubleshooting—Integrates syslog references to provide brief explanations and recommended actions for each message for isolating and resolving security issues quickly. The ASDM enables the parsing of syslog messages for customizable views based on time, date, syslog IDs, and IP

addresses. It also provides traceroute support for network connectivity testing and verification. An ASDM Assistance Guide provides task-oriented methods to configure features such as AAA, logging filters, and SSL VPN clients.